Testimony of David M. Barron

Chairman

Communications Sector Coordinating Council

The Future of Cyber and Telecommunications Security at The Department of Homeland Security

September 13, 2006

U.S. House of Representatives Committee on Homeland Security

Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity

Good Afternoon Mr. Chairman and fellow members of the committee. It is an honor to appear before you today and I thank you for the opportunity to discuss this very important topic, the future of cyber security and telecommunications.

I am David Barron, Assistant Vice President for Federal Relations/National Security with BellSouth Corporation here in our Washington office, but I am appearing today as the Chair of the Communications Sector Coordinating Council (CSCC). My testimony reflects my personal views as Chairman of the CSCC and not the views of Bell South.

Let me begin by giving you a brief background on the Sector Partnership Model and the Communications SCC in particular. Homeland Security Presidential Directive 7 (HSPD- 7) established the basis for a national coordinated approach to critical infrastructure protection, including the development of the National Infrastructure Protection Plan (NIPP) as well as the Sector Partnership Model. The NIPP defines the organizational structure that provides the framework for coordination of Critical Infrastructure and Key Resources (CI/KR) protection efforts at all levels of government, as well as within and across sectors.

Sector-specific planning and coordination are addressed through private sector and government coordinating councils that are established for each sector. Sector Coordinating Councils (SCCs) are comprised of private sector representatives. Government Coordinating Councils (GCCs) are comprised of representatives of the Sector-Specific Agencies, other Federal departments and agencies, and state, local, and tribal governments.

Established in 2005, the Communications Sector Coordinating Council has over 25 owner/operators and associations represented on the Council and we anticipate adding new members as we continue to broaden our membership. While HSPD-7 defined our sector as "Telecommunications", we in the industry feel that "Communications" is a more encompassing title that represents our diverse membership. Our membership today includes wireline, wireless, satellite, equipment manufacturers, and internet service providers among others. We are also actively trying to expand the membership to include cable telephony, emergency service providers and broadcasters so that our Communications Sector Coordinating Council truly represents the breadth of this dynamic sector; one of the sectors we call the "millisecond" sector due to the nature of how our sector works.

The CSCC is currently engaged in a wide variety of activities not only with our Communications Government Coordinating Council counterparts, but also with the Department of Homeland Security as well as other Sector Coordinating Councils on a number of initiatives, foremost of which is the creation of our Sector Specific Plan.

The NIPP base plan is supported by several Sector Specific Plans (SSPs) that provide further detail on how the critical infrastructure and key resources protection mission of each sector will be carried out. In late August the Communications SCC and GCC held a joint meeting in Washington, D.C. to coordinate on several issues, the most prominent of which is the development of the Sector-Specific Plan (SSP) as I mentioned before. The CSCC and GCC have been actively collaborating on a draft of the Communications SSP, with both Councils providing input and comments throughout the process. This effort is continuing and we are on track to submit the Communications SSP by the end of the year to DHS.

In addition to the SSP, the Communications SCC is engaged in several other important activities, including Pandemic Flu planning, National Coordinating Center (NCC) regional coordination, post-Katrina issues such as access, credentialing, and emergency responder status related to the Stafford Act, emergency wireless protocols, and many other activities.

Finally, the world of Communications often has considerable interaction and interdependencies with Information Technology (another critical infrastructure established by HSPD-7). As such, the Communications SCC has established a close relationship with the Information Technology SCC to work on issues of mutual concern. In September the Communications and Information Technology SCCs and GCCs will be holding the first ever Joint meeting, with all four councils present, to discuss cross-sector issues such as the creation of Sector Specific Plans that are complimentary and supportive of each other.

With the support of Under Secretary Foresman, Assistant Secretary for Infrastructure Protection Bob Stephan has overseen many of these initiatives while in the Acting Assistant Secretary for Cyber Security and

Telecommunications position and while serving as the Manager of the National Communications System (NCS). We are pleased with the progress that has been made. But the industry would welcome the additional focus brought to bear by a dedicated Assistant Secretary for Cyber Security and Telecommunications.

Obviously, we should view all the critical infrastructures and key resources defined in HSPD-7 as critically important to the nation. However, Communications and Information Technology is unique in that it underlies and supports all of the other sectors. Each of the other sectors depend upon computer systems, voice networks, broadband systems, wireless networks, and countless other structures and services provided by the Communications and IT communities. As a result, Congress has mandated and DHS has begun implementing strategies and procedures to ensure specific emphasis on these valuable cross-sector interdependencies. For example, the National Infrastructure Protection Plan and the supporting Sector Plans are working very specifically to address this convergence of Communications and Information Technology into what is referred to as the Next Generation Networks. As this work continues, there must be a balanced approach when looking at Cyber Security and Telecommunications. Both sectors are equally critical in support of the Nation's Homeland Security mission.

While DHS has been very helpful and responsive in many of these matters, there are areas in which the private sector would specifically like to see continued progress and improvement. First, while the current team of leadership at DHS, including Under Secretary Foresman, Deputy Under Secretary Robert Zitz, and Assistant Secretary Stephan, have done an excellent job, the position of Assistant Secretary for Cyber Security and Telecommunications remains vacant. As I stated earlier in my testimony, Assistant Secretary Stephan has done an admirable job in working with the Communications and Information Technology community but a dedicated Assistant Secretary could dramatically strengthen this critical public/private partnership.

Second, a clear definition of the mission needs to be established. What does Cyber Security and Telecommunications really mean as it relates to National Security, Homeland Security and Emergency Preparedness? In

other words, what is the problem that we are trying to solve? There is such a wide range of threats and vulnerabilities that a clear vision of the problem tied to priorities is essential.

Third, DHS needs to clearly define roles and responsibilities for all of those involved in this process. Again, this comes back to the understanding of the problem and a clear strategy based on risk assessment and priorities. By clarifying who is in charge of what, more will be accomplished in an efficient and effective manner.

Finally, DHS should recognize that the private sector is willing and fully committed to this partnership. If this framework is truly intended to be a partnership, then more emphasis needs to be placed on ensuring there is a trusted relationship between the public and private sectors, which is in the best interest of our Nation's security. For example, the National Coordinating Center for Communications – the NCC – is a model to follow for the partnership that is mandated by the future. In the NCC, government and industry sit together everyday to prepare for and to respond to events that threaten the Nation's communications networks. The NCC has had a long history of success and I think this model could and should be expanded to include other infrastructures like Information Technology/Cyber and Electric Power. The continued health and evolution of the partnership depends not only on private sector participation, but DHS' s recognition of the value of that partnership with a commitment to work more closely with industry.

As I close, I would like to again thank Congress for the opportunity to speak today and for their support in these efforts. The partnership framework is incredibly valuable and continues to serve as a conduit for unprecedented cooperation and collaboration between government and private industry. There is room for improvement to be sure, but the suggestions I have presented here today are intended to further strengthen these valued interactions and ensure we jointly continue to take steps to secure our homeland.

Thank You.